Proof Systems and Satisfiability problem

Anahit, Chubaryan
Yerevan State University
Yerevan, Armenia
e-mail: achubaryan@ysu.am

Armen, Mnatsakanyan
Yerevan State University
Yerevan, Armenia
e-mail: arm.mnats@gmail.com

ABSTRACT
Various proof complexity characteristics are investigated in three propositional proof systems, based on determinative disjunctive normal forms. The comparative analysis for size, time, space, width of proofs is given. These results can be used for Satisfiability problem solving.

Keywords
Determinative conjunct, determinative disjunctive normal form, elimination rule, size, time, space, width of proofs.

1. INTRODUCTION
One of the most fundamental problems of the proof complexity theory is to find a n e fficient p roof s ystem for propositional calculus. During the last decade an active line of research in classical propositional proof complexity was carried out to study space complexity and size-time-space-width trade-offs for proofs. The space of proving a formula corresponds to the minimal size of a black-board needed to verify all steps in the proof. Besides being an interesting natural complexity measure, space has connection to the memory consumption of SATIS-FIABILITY (SAT) problem solving, and so research has mostly focused on weak systems that are used by SAT solvers.

Using the notion of determinative disjunctive normal form (dDNF), introduced by the first coauthor in [1] and two proof systems introduced in [2] on the base of dDNF, we also describe a new propositional proof systems. We use all three systems for SAT problem solving and in-vestigate the comparative analysis for the mentioned proof complexity characteristics in them.

It is known that some of complexity measures (for example space and time) sometimes display a trade-o : there are formulas having proofs in both short length and small space, but for which there cannot exist proofs in short length and small space simultaneously. For our systems we obtain the simultaneous bounds for different measures.

The upper bounds for size, time, space and width are obtained on the base of some normal forms of proofs in the mentioned systems. The "good" lower bounds are obtained using the sequence of some tautologies.

2. MAIN NOTIONS AND NOTATIONS
We use the well-known notions of the unit Boolean cube (E^n), propositional formula with the logical connectives $\neg$, $\&$, $\vee$, $\supset$, a tautology, a proof system for classical propositional logic [3].

2.1 Determinative disjunctive normal form
Following the usual terminology we call the variables and negated variables *literals*. The conjunct K can be represented simply as a set of literals (no conjunct contains a variable and its negation simultaneously).

In [1] the following notions were introduced.

We call a *replacement-rule* each of the following trivial identities for a propositional formula ψ:

$$\begin{array}{llll} 0\&\psi = 0, & \psi\&0 = 0, & 1\&\psi = \psi, & \psi\&1 = \psi, \\ 0 \vee \psi = \psi, & \psi \vee 0 = \psi, & 1 \vee \psi = 1, & \psi \vee 1 = 1, \\ 0 \supset \psi = 1, & \psi \supset 0 = \overline{\psi}, & 1 \supset \psi = \psi, & \psi \supset 1 = 1, \\ \overline{0} = 1, & \overline{1} = 0, & \overline{\overline{\psi}} = \psi. & \end{array}$$

Application of a replacement-rule to some word consists in replacing some of its subwords, having the form of the left-hand side of one of the above identities, by the cor-responding right-hand side.

Let φ be a propositional formula, $P = \{p_1, p_2, \ldots, p_n\}$ be the set of all variables of φ, and $P' = \{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$ $(1 \leq m \leq n)$ be some subset of P.

Definition 1. *Given $\sigma = \{\sigma_1, \ldots, \sigma_m\} \subset E^m$, the conjunct $K^\sigma = \left\{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\right\}$[1] is called $\varphi - 1$-determinative ($\varphi - 0$-determinative) if assigning σ_j ($1 \leq j \leq m$) to each p_{i_j} and successively using replacement-rules we obtain the value of φ (1 or 0) independently of the values of the remaining variables.*

$\varphi - 1$-determinative conjunct and $\varphi - 0$-determinative conjunct are called also φ-determinative or determinative for φ.

Definition 2. *DNF $D = \{K_1, K_2, \ldots, K_l\}$ is called determinative DNF ($dDNF$) for φ if $\varphi = D$ and every conjunct K_j $(1 \leq i \leq j)$ is 1-determinative for φ.*

It is obvious that for every propositional formula φ perfect DNF is φ-determinative.

[1] As usual, given a propositional variable p and $\sigma \in E^1$, by p^σ we denote the function $p^\sigma = \begin{cases} p, & \text{if } \sigma = 1, \\ \overline{p}, & \text{if } \sigma = 0. \end{cases}$

2.2 Main systems

2.2.1 Elimination system E

This system is introduced in [2]. The axioms of E aren't fixed, but for every formula φ each conjunct from some $dDNF$ of φ can be considered as an axiom.

The *elimination rule* (ε-rule) infers $K' \cup K''$ from conjuncts $K' \cup \{p\}$ and $K' \cup \{\overline{p}\}$, where K' and K'' are conjuncts and p is a variable.

The proof in E is a finite sequence of conjuncts such that every conjunct in the sequence is one of the axioms of E, or is inferred from earlier conjuncts in the sequence by ε-rule.

DNF $D = \{K_1, K_2, \ldots, K_l\}$ is tautology if using ε-rule can prove the empty conjunct ($\emptyset$) from the axioms $\{K_1, K_2, \ldots, K_l\}$.

2.2.2 Cut-free Frege system $\mathcal{F}^-$

This system is introduced also in [2]. The schematic axioms of the system $\mathcal{F}^-$ are the following:

I $\alpha_1 \& (\alpha_2 \& \ldots \& (\alpha_{m-1} \& \alpha_m) \ldots) \supset \alpha_i$, $m \geq 1$, $1 \leq i \leq m$,

II 1. $(K \supset \alpha) \supset ((K \supset \neg\beta) \supset (K \supset \neg(\alpha \supset \beta)))$
2. $(K \supset \neg\alpha) \supset (K \supset (\alpha \supset \beta))$
3. $(K \supset \beta) \supset (K \supset (\alpha \supset \beta))$
4. $(K \supset \alpha) \supset ((K \supset \beta) \supset (K \supset \alpha \& \beta))$
5. $(K \supset \neg\alpha) \supset (K \supset \neg(\alpha \& \beta))$
6. $(K \supset \neg\beta) \supset (K \supset \neg(\alpha \& \beta))$
7. $(K \supset \neg\alpha) \supset ((K \supset \neg\beta) \supset (K \supset \neg(\alpha \vee \beta)))$
8. $(K \supset \alpha) \supset (K \supset \alpha \vee \beta)$
9. $(K \supset \beta) \supset (K \supset \alpha \vee \beta)$
10. $(K \supset \alpha) \supset (K \supset \neg\neg\alpha)$

III 1. $(\delta \& K \supset \varphi) \supset ((\overline{\delta} \& K \supset \varphi) \supset (K \supset \varphi))$
2. $(\gamma \supset \varphi) \supset ((\overline{\gamma} \supset \varphi) \supset \varphi)$,

where

a) φ is a provable formula,

b) α_i ($1 \leq i \leq m$) and γ are literals, α, β, δ are arbitrary formulas,

c) $K = \beta_1 \& (\beta_2 \& \ldots \& (\beta_{l-1} \& \beta_l) \ldots)$ ($l \geq 1$) for arbitrary literals β_i ($1 \leq i \leq l$),

d) for every $\beta_1 \& (\beta_2 \& \ldots \& (\beta_{l-1} \& \beta_l) \ldots) \supset \varphi$ style subformula from some axiom of second group conjunct $\{\beta_1, \ldots, \beta_l\}$ is φ-determinable,

e) if $K^{set} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ for some subformula $K = \beta_1 \& \beta_2 \& \ldots \& \beta_k$ from first axiom of third group, then $\delta \notin K^{set}$ and $\{\delta\} \cup K^{set}$ is subset of some φ-determinative conjunct, but K^{set} is not φ-determinative.

Rule of inference is modus ponens $\frac{A \quad A \supset B}{B}$. Note that these systems "repeat" Calmar's method of classical Frege systems completeness proof.

2.2.3 The system E(lin)

Now we describe some new proof system, based on dDNF. Let for some formula φ $K = \{p_{i1}^{\sigma_1}, p_{i2}^{\sigma_2}, ..., p_{im}^{\sigma_m}\}$ be $\varphi-1$-determinative conjunct. By K^0 we denote equation $\sum_{j=1}^{m} \alpha(p_{ij}^{\sigma_j}) = 0$, where

$$\alpha(p_{ij}^{\sigma_j}) = \begin{cases} x_{ij} & \text{if } \sigma_j = 1 \\ 1 - x_{ij} & \text{if } \sigma_j = 0 \end{cases}$$

If φ is the propositional formula in n variables and $D = \{K_1, K_2, \ldots, K_l\}$ is dDNF for φ, then as axioms of E(lin) we consider the system

$$\begin{cases} x_i = 0 \vee x_i = 1 & 1 \leq i \leq n \text{ (Boolean axioms)} \\ K_j^0 & 1 \leq j \leq l \end{cases}$$

Note that if φ is tautology, then this system is unsatisfiable. As inference rules we consider the inference rules of the system R(lin) [4]:
Resolution. Let A,B be two disjunctions of linear equations (possibly the empty disjunctions) and let L_1, L_2 be two linear equations. From $A \vee L_1$ and $B \vee L_2$ derive $A \vee B \vee (L_1 + L_2)$ (+resolution) or $A \vee B \vee (L_1 - L_2)$ (-resolution).
Weakening. From a disjunction of linear equations A derive $A \vee L$, where L is an arbitrary linear equation.
Simplification. From $A \vee (0 = k)$ derive A, where A is a disjunction of linear equations and $(k \neq 0)$. An E(lin) refutation of a formula φ is a proof of the empty disjunction from the above constructed system.
We shall sometimes speak about refutation and proofs interchanging.

2.3 Proof complexity measures

In the theory of proof complexity two main characteristics of the proof are: $t - complexity$, defined a s the number of proof steps (time) and $l - complexity$, defined as total number of proof symbols (size). Now we also consider two measures (space and width). $s - complexity$ (space), defined a s m aximum o f minimal number of symbols on blackboard needed to verify all steps in the proof and $w - complexity$ (width), defined as the maximum of widths of proof formulas. Note that formal definitions are for example in [5].
Let Φ be a proof system and φ be a tautology. We denote by $t_\varphi^\Phi(l_\varphi^\Phi, s_\varphi^\Phi, w_\varphi^\Phi)$ the minimal possible value of $t - complexity(l-complexity, s-complexity, w-complexity)$ for all proofs of tautology φ in Φ.
Some results on $t - complexity$ and $l - complexity$ are obtained for the systems E and $\mathcal{F}^-$ in [2]. Here we add the results on $s - complexity$ and $w - complexity$ measures and also investigate them in the system E(lin).

3. MAIN RESULTS

In further consideration the following tautologies (Topsy-Turvy Matrix) play a key role

$$TTM_{n,m} = \vee_{(\sigma_1,\ldots,\sigma_n) \in E^n} \ \&_{j=1}^{m} \ \vee_{i=1}^{n} p_{ij}^{\sigma_i}$$

$$(n \geq 1, 1 \leq m \leq 2^n - 1).$$

For all fixed $n \geq 1$ and m in above-indicated intervals every formula of this kind expresses the following true statement: given a 0,1-matrix of order n x m we can topsy-turvy some strings (writing 0 instead of 1 and 1 instead of 0) so that each column will contain at least one 1.
Note that the minimal number literals in any determinative conjunct of $TTM_{n,m}$ has at least 2^m conjuncts.

Let $\varphi_n = T\,TM_{n,2^n-1}$. By $|\varphi|$ we denote the size of a formula φ (or some of its presentation), defined as the number of all variable entries. It is obvious that the full length of a formula, which is understood to be the number of all symbols or the number of all entries of logical signs, is bounded by some linear function in $|\varphi|$. $|\varphi_n| = n2^n(2^n-1)$ and $\log|\varphi_n| = \Theta(n)$

Theorem 1. *Let* Φ *be one of the systems* $E, \mathcal{F}^-, E(lin)$ *then*

$$\log_2\log_2 t^{\Phi}_{\varphi_n} = \Theta(n)$$
$$\log_2\log_2 l^{\Phi}_{\varphi_n} = \Theta(n)$$
$$\log_2 w^{\Phi}_{\varphi_n} = \Theta(n)$$
$$\log_2 s^{\Phi}_{\varphi_n} = \Theta(n)$$

The upper bounds are obtained on the base of perfect disjunctive normal form for φ_n.
The lower bounds are obtained on the base of some properties of proofs giving for φ_n in the system E and $\mathcal{F}^-$ [2]. The same properties are valid for the proof, given in $E(lin)$.

4. ACKNOWLEDGEMENT

This work is supported by Grant number 13-1b004 of SCS of RA.

REFERENCES

[1] An. Chubaryan, Arm. Chubaryan, "A new conception of Equality of Tautologies", *L &PS, Vol. V, No 1*, pp. 3-8, 2007.

[2] An. Chubaryan, "Comparative efficiency of some proof systems for classical propositional logic", *Journal of CMA (AAS),v.37, N5*, pp. 71-84, 2002.

[3] S.A.Cook, A.R.Reckhow, "The relative efficiency of propositional proof systems", *Journal of Symbolic Logic, vol. 44*, pp. 36-50, 1979.

[4] Ran Raz, Iddo Tzameret, "Resolution over linear equations and multilinear proofs", *Ann. Pure Appl. Logic 155(3)*, pp. 194-224, 2008.

[5] Y. Filmus, M. Lauria, J. Nordstrom, N. Thapen, N. Ron-Zewi "Space Complexity in Polynomial Calculus", *2012 IEEE Conference on Computational Complexity (CCC)*, pp. 334-344, 2012.